Password Policy for MFASIS Accounting

Identification and Authentication

Each person who is granted access to the statewide accounting system is assigned a unique personal identifier or User ID.

If the user's employment or job responsibilities change, the user's authorization to access the Accounting system must be removed or modified accordingly. The employee's supervisor must notify their Agency Security Coordinator and the Controller's Security Administrator to appropriately modify the employee's security privileges.

Each user is authenticated before access to information is granted. Authentication is performed by using a password system, in conjunction with the User ID.

Password Management

The BIS Helpdesk (624-7700) is responsible for resetting passwords for the MFASIS Accounting system.

Password Aging

You should change your password every 30 days. Your User ID will be automatically disabled if it has not been changed in a 120-day period. Your User ID will be deleted after 6 months of non-use.

Password History

The system maintains a history of the twelve most recent passwords. You may not re-use a password more frequently than every 360 days.

Account Lockout

When you enter an incorrect User ID/password, you will receive a message stating that the sign-on attempt was unsuccessful. You are then required to correctly re-enter your User ID and password. If you fail to log on correctly after three attempts, your access is automatically revoked.

Reinstating a User ID

If your access is revoked due to incorrect sign-on attempts, contact the BIS Helpdesk (624-7700) to reinstate your security. Your Agency Security Coordinator is responsible for verifying your identity. You must change your temporary password to a password of your choosing the first time you sign on.

Protecting Your Password

You **must maintain exclusive control of your password** and protect it from inadvertent disclosure to others.

Do not share your password with anyone. If you know of an instance where a password has been shared, report the incident to the Controller's Security Administrator at 626-8427.

If you knowingly share your ID and password with another user, and the incident comes to the attention of your security coordinator or other security administrator, your User ID will be immediately de-activated. Depending on the circumstances, your User ID may be revoked. You will then need to re-apply for access to MFASIS Accounting, and may or may not be given the same security level.

You, as the owner of your User ID and password, are responsible for any unauthorized activity accomplished using your User ID and password. If there is a possibility that your ID has been compromised, change your password immediately and notify your supervisor.

No Macros or F keys

Do not develop a macro or assign an F key to "remember" your password. Using this method to sign on is considered a security breach.